Experimental Security Panoramas Workshop

DARPA Initiatives in the Cyber Experimentation Domain

National Cyber Range (NCR)

Lt Col David Robinson, PhD

14 July 2011

Mr. Don Woodbury
Director, STO
703-696-2362
donald.woodbury@darpa.mil

Strategic Technology Office

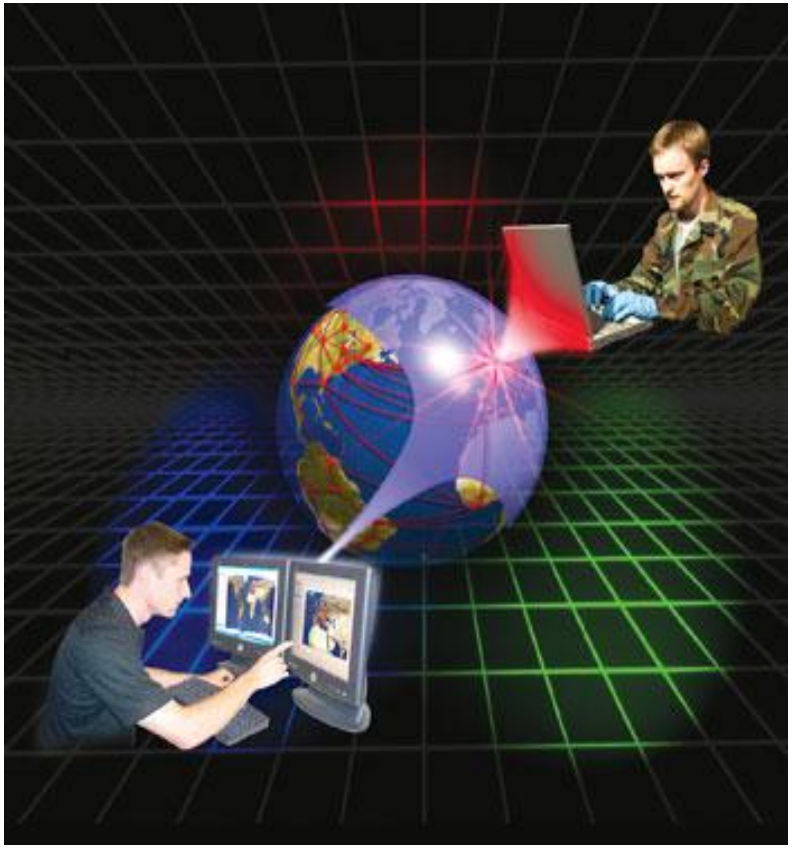
Dr. Brent Appleby
Deputy Director, STO
703-248-1531
brent.appleby@darpa.mil

Dr. Larry Stotts
Deputy Director, STO
571-218-4346
larry.stotts@darpa.mil

Approved for Public Release, Distribution Unlimited

Cyber Threat Summary

- **Loss of military technological advantages:** The continued exploitation of information networks and the compromise of sensitive/classified data needs to be addressed to ensure the United States military's technological advantage.
- **Loss of U.S. economic value:** Losses from intellectual property due to data theft in 2008 are estimated at $1 trillion.
- **Failure of critical infrastructures:** The intelligence community has concluded that a number of nations already have the technical capability to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures.
- **Exploitation of global financial services:** Data breach of a U.S. retailer resulted in the loss of personally identifiable information affecting 45 million credit and debit cards.



Approved for Public Release, Distribution Unlimited
Distribution authorized to U.S. government agencies only.

National Cyber Range Program Overview

Background:

- Comprehensive National Cybersecurity Initiative (NSPD-54)
  - "To establish a front line of defense against today's immediate threats by **creating or enhancing…the ability to act quickly** to reduce our current vulnerabilities and prevent intrusions."
  - To "develop **enduring 'leap-ahead' technology**…that provide[s] increases in cybersecurity by orders of magnitude above current systems and which can be deployed within 5 to 10 years." (Initiative 9).

NCR Program Goals: Develop the technologies (NOT just another range) for advanced cyber research and testing

- Hardware and software automation tools that allow a range to be rapidly configured to emulate complex, large-scale heterogeneous networks
- Software tools and sensors that allow cyber threats (e.g. worm or virus) to be thoroughly studied, providing a fundamental understanding of their behavior and potential defense mechanisms
- Decrease the time required to sanitize and reconfigure the range after testing to decrease downtime between tests
- Enable multiple, independent, simultaneous, multi-security level experiments, from TS/SCI to unclassified, on the same infrastructure to maximize the range utilization
- Simplify the process of introducing and testing new code on a cyber range

The National Cyber Range seeks to enable experimentation to address the growing cyber threat in a manner that is more thorough, quicker, and cost effective than existing ranges.

Approved for Public Release, Distribution Unlimited

National Cyber Range Objectives and Challenges

Enable leap-ahead technologies through:

- Development of revolutionary cyber-security experimentation technologies
- Development of revolutionary automated range configuration technologies
- Development of innovative experimentation-specific technologies
- Delivery of technologies to existing and future ranges and communities

Challenges

- Develop technologies that currently do not exist
- Scale experiments and technologies
- Replicate desired systems within physical and time constraints

Approved for Public Release, Distribution Unlimited

NCR Technical Approach

Automated Range Management

- Multiple, independent, simultaneous experiments
- Simultaneous Unclassified to Top Secret/Special Compartmentalized Experiments

Automated Experiment Management

- Design, configure, monitor, analyze, and release experiments with interactive experiment suite
- Experiment toolkit/repository for reuse of recipes and architectures

Node Replication

- Rapidly generate and integrate replications of new machines
- Forensic data collection across range without impacting experiments
- Sanitize machines within minutes rather than hours

Research Focused

- Implements a scientific method for rigorous cyber experimentation
- Easily integrate revolutionary research systems
- Connect securely to existing special purpose ranges
- Realistic experiments of Internet/Global Information Grid scale research
- Rapidly integrate new research protocols across the protocol stack

Human Interaction and Replication

- Realistically replicate adaptive human network behavior

Security Requirements

- Encapsulate and isolate experiments, data storage, and networks
- Unclassified to TS/SCI/SAP

Approved for Public Release, Distribution Unlimited

NCR Technologies

Cyber Foundation	Range Management	Experiment Management
• Cyber Scientific Method • Cyber Scientific Experiment Language Specification—schema used to capture every aspect of an experiment • Asset Characterization • Asset Description Specification and Database Specifications • Security Management Design • Experiment Design using Statistical Methods • Network Configuration Design Input • Leverage of additional protocols, services and networks	• Knowledge Management Suite • Facility Management Suite • Experiment Specification Tools • Automated Pre-Experiment Planning • Automated Resource Allocation --- • Rapid and Secure Resource De-obligation after Experiments • Efficient Free Resource Pooling • Lessons Learned Knowledge Management Suite • Incorporation of Additional Technologies into the Range • Sanitization Toolset	• Automated Range Configuration, Validation and Experiment Close-Out • Development of Instrumentation for Data Collection • Automated Experiment Control and Management • Automated Data Analysis and Presentation Tools • Recall of Previous Experiments, Results and Data Analysis • Semi-Automated Library of Offensive and Defensive Tools • Automated Reconstitution of Experiments • Real Time Human Interaction (Real and Simulated) with Experiments

Approved for Public Release, Distribution Unlimited

NCR Two Performers – Two Designs – Some Commonality

OnPath Layer One Network Switch

- Electronic Patch Panel
- Tested By Sandia National Labs
- All network assets can be quickly reconfigured to meet follow-on requirements

Data At Rest - Encryption Is The Key

- Performers are using Suite B NSA Encryption Technologies
- Data at rest is Encrypted and Considered Cyphertext
- Hard Drives Never Have Classified Data On Board
- No Traditional Destruction Required
  - Drives will still be destroyed as classified at end of life

Sanitization

- Server Sanitization
  - Both performers have well engineered sanitization plans
    - Sanitizing **ALL** Memory "as required" during experiments
    - **ALL** memory will be sanitized at the end of experiments
  - Both performers have worked closely with vendors for highly detailed statements of volatility.

Approved for Public Release, Distribution Unlimited

NCR Hardware and Current Status

Two performers are developing range prototypes:

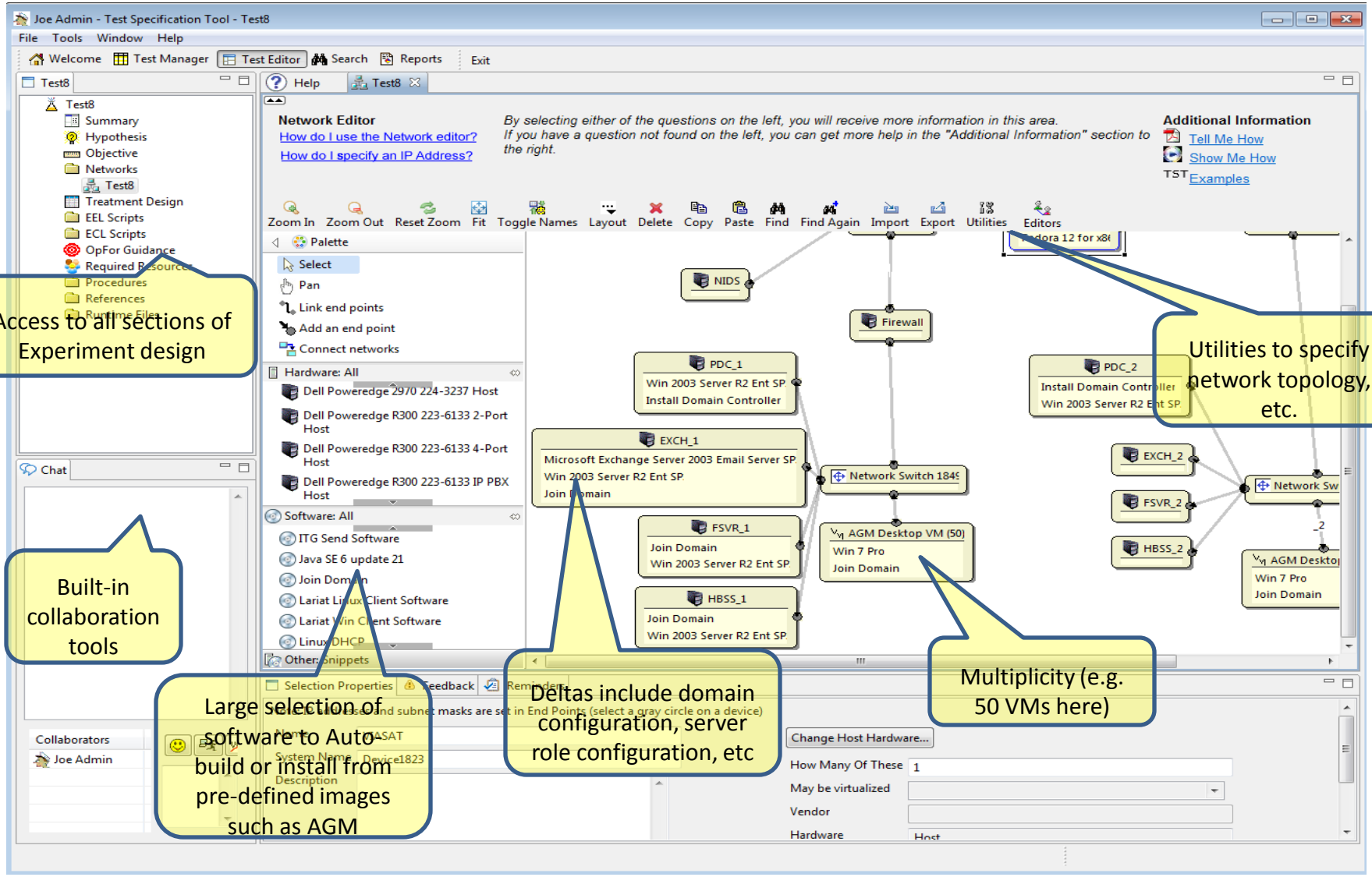
- Lockheed Martin
  - 220 node range, able to emulate > 2000 users
- John Hopkins Applied Physics Laboratory
  - 50 node range, able to emulate > 500 users

Common system features

- Layer-1 network switch
  - Electronic patch panel for rapid and automated range configuration and reset
- Encrypted data at rest
  - Data at rest is encrypted and considered cyphertext (Suite B NSA encryption technologies)
  - Hard drives never contain classified data
  - No traditional sanitization or destruction of magnetic media required
- Range sanitization
  - All memory, including non-volatile memory, sanitized at the end of experiments
  - Hard-drive sanitized by clearing encryption keys

Approved for Public Release, Distribution Unlimited

Lockheed Martin Test Specification Tool



Drag and Drop experiment design with interface similar to Microsoft Visio.

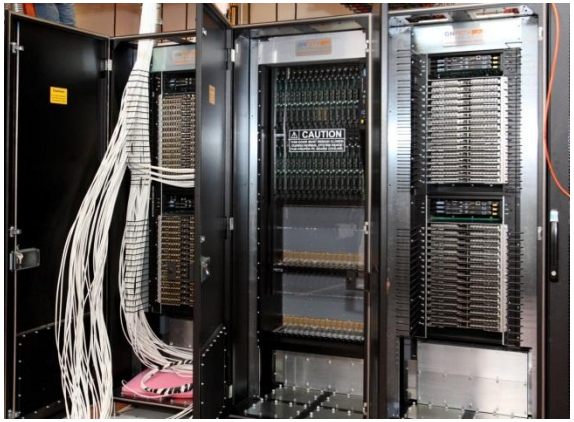
Approved for Public Release, Distribution Unlimited

NCR Significant Accomplishments

- **Development of Two Operational Prototypes**
  - Johns Hopkins University Applied Physics Laboratory (JHU/APL
    - Operating Procedures 100% complete
    - 100 % of hardware integrated
    - 4 million Software Lines of Code integrated
    - Integration Testing 85% complete
    - SCI Facility is 100% complete—still requires equipment move
    - Interactive Test Suites 100% complete
  - Lockheed Martin (LM) NCR Range
    - Operating Procedures 100% complete
    - 100 % of hardware integrated
    - 5 million Software Lines of Code integrated
    - Integration Testing 90% complete
    - SCI Facility is 100% complete—no equipment move required
    - Interactive Test Suites 100% Complete
  - Certification and Accreditation (C&A) to operate from Unclassified to Top Secret levels
    - Documentation 90% complete
    - C&A Component and End-to-End Testing 100% complete

- **Development of Key Technologies**
  - Automatic experiment planning/design 95% complete
  - Automatic creation of new node configurations 90% complete
  - Automated range configuration/validation 100% complete
  - Controlled Interfaces are 100% complete
  - Automated sanitization 90% complete
  - Virtual machine development 90% complete
  - Time Synchronization capability 100% complete
  - High fidelity traffic generation 90% complete
  - Experiment Control is 100% complete
  - Data Analysis System is 80% complete
  - Visualization of experiment results is 90% complete

Layer-1 Switch Front

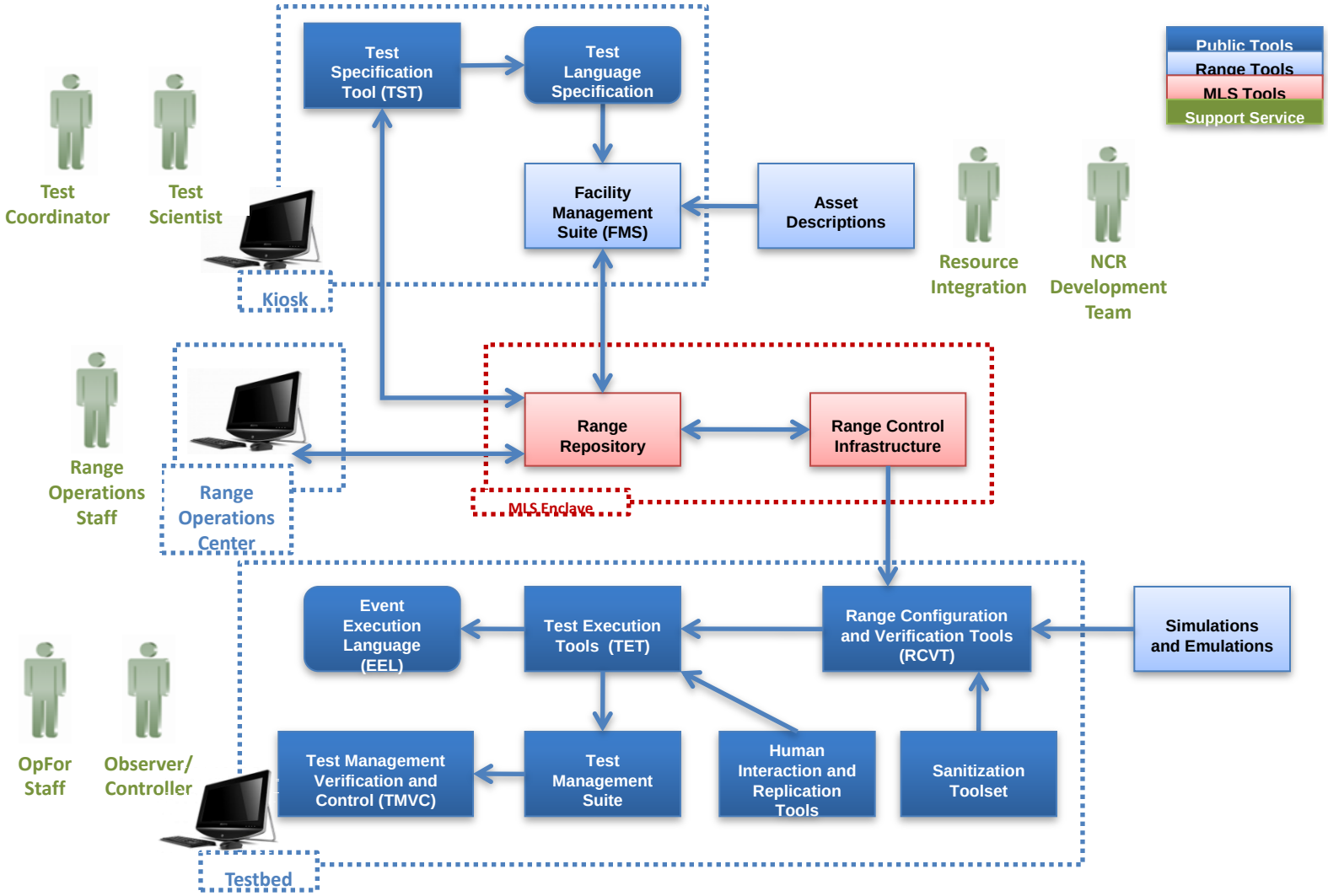


Layer-1 Switch Back

Layer-1 Switch, enabling automated range configuration, has completed physical integration, software control development and initial testing.

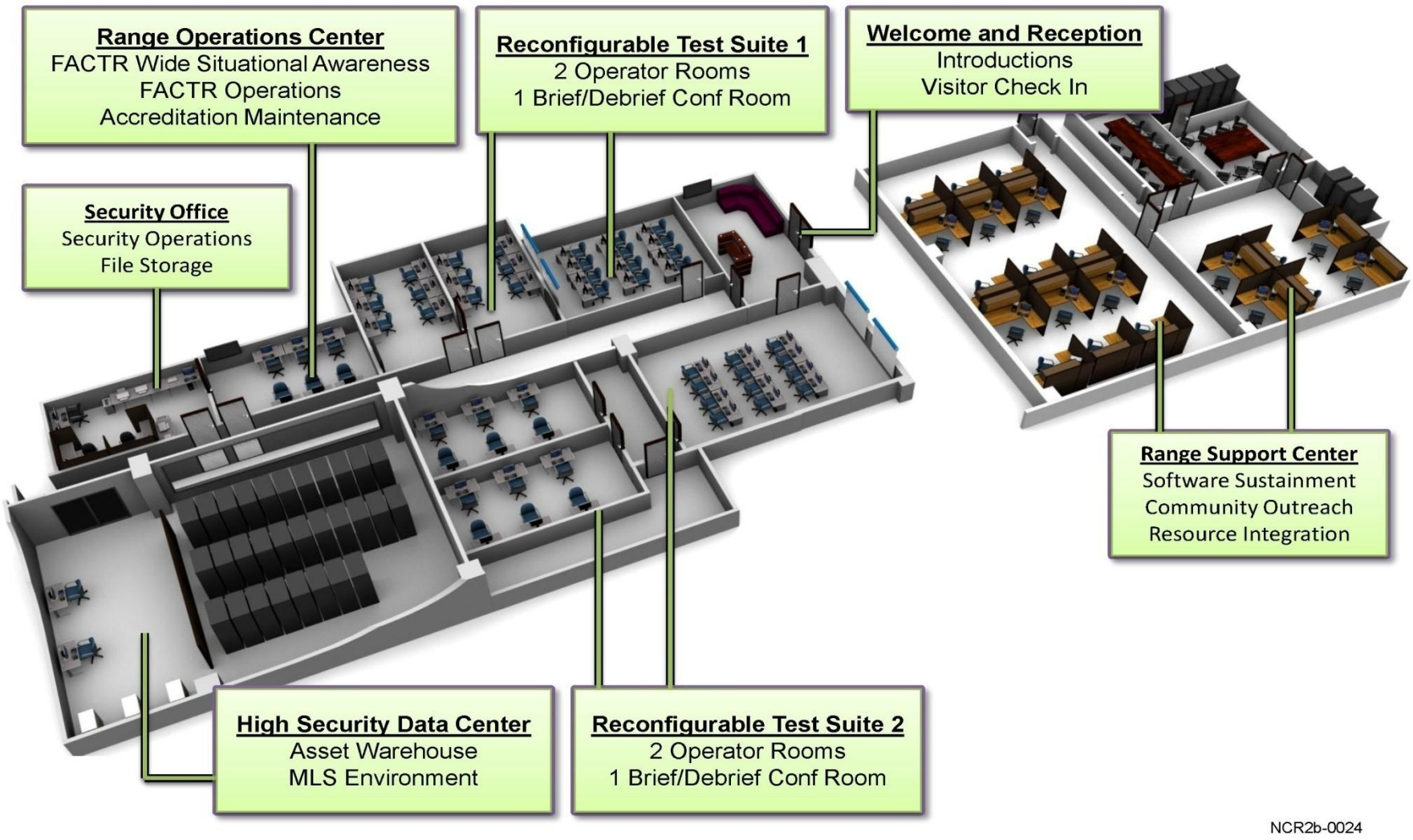
Approved for Public Release, Distribution Unlimited

NCR Overview – Logical Architecture



Approved for Public Release, Distribution Unlimited

Prototype NCR facility



Approved for Public Release, Distribution Unlimited

NCR Use Case Examples and Capabilities

- Advanced cyber research and new capability development
- Testing of network protocols, policies, and vulnerabilities
- Analysis of malware collected targeting national interests
- Providing simulated and emulated environments for mission critical software upgrades on national assets
- Source selection testing for network hardware and software procurements
- Cyber training and exercises
- Secure cloud computing and storage architecture

Approved for Public Release, Distribution Unlimited
Distribution authorized to U.S. government agencies only

NCR Use Case Examples and Capabilities

- Testing New Offensive and Defensive Cyber Technologies
  - NCR provides the ability to rapidly design and conduct tests with realistic network topologies and software configurations
  - Malicious new code can be introduced onto the range without fear of compromising range security

- Testing New and Advanced Network Protocols
  - Ability to scale range size to > 2000 users to emulate large enclaves
  - The NCR can emulate test networks with network nodes (workstations and servers) in linear, mesh, star, or custom network topologies
  - The range supports a diverse set of Linux and Window's based operating systems, patch levels, and configurations. The NCR tools provide the ability to build new host configurations on the fly
  - NCR's diverse traffic generation systems can provide required traffic for testing:
    - High data rate legacy (e.g., HTTP, SMTP, FTP, etc.) traffic
    - Malicious background traffic and automated port scanning and attack traffic

Approved for Public Release, Distribution Unlimited
Distribution authorized to U.S. government agencies only

NCR Use Case Examples and Capabilities

- Malware Analysis
  - Testing for analysis of malware collected by various DoD response teams, the Joint Malware Catalog, and US-CERT (all currently conducts small scale testing)
  - Precise specification of OS, patches, and application software on target system
  - High test replication fidelity through full coordinated scripting and automation tools
  - Pause, resume, and rapid restore functionality allow for iterative testing
  - High fidelity sensors and a full measurement framework for adding new sensors

- Simulation Environment for National Asset Command and Control
  - Test mission critical software upgrades and security profiles on simulations of national assets which cannot actually be taken off-line

- Enterprise-wide Solutions Steering Group (ESSG) RFP Source Selection Testing
  - The ESSG procures DoD wide licenses for anti-virus, HBSS, firewalls, and similar products. Reduced test design and testbed build times allow for more testing on each potential solution
  - Use of pre-configured standard images on the NCR (USN COMPOSE, Army Gold Master, USAF Standard Desktop) allow for more DoD relevant test results.
  - Vetting procurements on the NCE would allow for services, CoComs, and other interested parties to observe and participate as required

Approved for Public Release, Distribution Unlimited
Distribution authorized to U.S. government agencies only

NCR Use Case Examples and Capabilities

- Training and Exercises
  - The NCR is capable of hosting:
    - Defensive exercises like CDX (USMA, USNA, USAFA, AFIT, NPS annual exercise)
    - Offensive training such as cyber capture the flag exercises for war fighters
  - The NCR provides advanced measurement and visualization tools for cyber event coordinators
  - A full compliment of sensor suite are available that allow for both simple and complex metrics and measures of participant performance without interfering with their workflow
  - The diverse set of advanced traffic generation tools on the NCR can be used to provide cover for red teams
  - NCR provides the ability to pause operation and to rapidly revert to a check point, allowing for immediate feedback to reinforce lessons learned and repeat failed events

- Secure cloud computing and storage architecture
  - The NCR architecture represents a MLS cloud computing and storage facility. The range tools can be used in future cloud architectures as well as cloud security testing

Approved for Public Release, Distribution Unlimited
Distribution authorized to U.S. government agencies only

NCR Program Schedule

- Phase I (Q2 2009 – Q4 2009)
  - Develop initial design and concept of operation
- Phase II (Q2 2010—Q4 2011)
  - Complete the design and demonstrate range technologies
  - Modified in November 2010 to complete an operational prototype
    - Independently verify and validate range technologies
    - Certify and accredit range to operate at multiple security levels (DNI)
- Phase II-B (Q4 2011—Q4 2012)
  - Operation/testing of the prototype NCR
  - Enhance existing software tools and ensure the range hardware and software are stable to allow for a seamless transition
  - Develop business model for sustainable range operation and expansion beyond FY12
  - Transition the range and associated technologies

Approved for Public Release, Distribution Unlimited

NCR Phase II-B Objectives and Approach

Phase II-B: DARPA will operate the NCR during Phase II-B (12 month) beginning in Fall 2011. DARPA and the NCR Management Transition Partner will work together to demonstrate the technologies developed during Phase II and to conduct real experiments.

Phase II-B Objectives:

- Establish and execute a portfolio of experiments and range use cases
- Demonstrate the advanced technologies developed in Phase II to the cyber community
- Develop business models for sustainable range operation and expansion beyond FY12

Phase II-B Prototype Operation Approach:

- Refine Prototype operation to minimize time required to execute experiments
- Correct any software/hardware issues that prevent Prototype operation and transition
- Establish and execute a portfolio of experiments supporting cyber development that other agencies can leverage in the cyber experiments
- Complete (if not accomplished in Phase II) and maintain Certification and Accreditation of the Prototype
- Document experiment/demonstration results including significant NCR unique successes and significant Prototype shortcomings
- Transition NCR Prototype software tools to other existing ranges

Approved for Public Release, Distribution Unlimited

Summary

Challenge	Current Ranges	National Cyber Range (Planned)
Range Application	• Testing in a degraded environment and information assurance • Generalized behavior of cyber tools • Security often prevents the introduction of new code	• Develop new and untested capabilities • Ability to introduce and execute new code • Understand the fundamental behavior of new tools • Rapid reset and reuse of range to allow for multiple tests of simple thought experiments
Security	• Single test at single security level	• Multiple simultaneous experiments at different security levels
Rapid Testbed & Test Configuration	• Manual configuration of hardware and tests with scripts	• Automated configuration of hardware and experiments • Range design tool to design experiments, configure testbed resources, and manage testbed assets
Network and User Realism	• Tradeoff between physical (realism) and scale (emulation) • Statistical traffic generators	• Large-scale combinations of physical and virtual systems • Diverse device emulation • Traffic generators that more realistically emulate human behavior
Rapid Testbed Recovery	• Primarily single-use	• Automated range sanitization in order to support re-use of testbed assets

The NCR key features:

- **Automated range configuration to simulate diverse network profiles**
- **Automated range sanitization (hard-drives, NVRAM)**
- **Custom network performance sensors**
- **Ability to run multiple simultaneous experiments at different security levels**
- **Simplified ability to introduce, execute, and test new (malicious) code**